IN THE SPECIFICATION:

Replace the paragraph beginning at page 26, line 4 with the following paragraph:

A "pattern testing" attack of the type described above can also be prevented in accordance with the present invention by imposing additional mathematical constraints (such as maximum run-lengths), e.g., constraints beyond those specified by the HDCP protocol, on the key selection vector values employed during authentication exchanges, and implementing each receiver and transmitter to test each key selection vector that it receives during each authentication exchange for compliance with each additional such mathematical constraint. For example, in one embodiment, a receiver or transmitter (of a system implementing the HDCP protocol) is implemented to test each key selection vector that it receives during each authentication exchange (e.g., in KSV checking logic circuitry 187A ~~187~~ shown in Fig. 7) for compliance with at least one additional mathematical constraint beyond the constraints specified by the HDCP protocol.

Replace the paragraph beginning at page 35, line 32 with the following paragraph:

Among the ways to prevent such attacks (in which the same transmitter is used to encrypt and decrypt the data of interest) in accordance with the invention are the following:

the transmitter is implemented so that, after it has entered an initial state determined by the shared secret "Km" and a value "An" (after undergoing an authentication exchange) and then encrypted a set of data, it is difficult or impossible for an attacker to place the transmitter in the same initial state. One way to accomplish this is to introduce additional randomness into the process by which the transmitter generates the value "An" prior to encrypting data. Introducing a gaussian analog effect into the pseudo-random function employed to generate "An" would make it more difficult for an attacker to cause the transmitter to generate the same "An" value during both phases of the attack. One way to do this is to incorporate a diode-based white noise source into the "An" value generation process (e.g., to include such a noise source in "An" value generation circuitry 192A ~~192~~ in transmitter 190 of Fig. 8). Another way is to require that the transmitter employ an R-C oscillator (i.e., one affected in significant but difficult-to-predict ways by system temperature, voltage, noise, and other physical forces) to generate a variable count or time delay during the process of generating the "An" value (e.g., to include such an oscillator in "An" value generation circuitry 192A ~~192~~ in transmitter 190 of Fig. 8). Alternatively (or additionally), any of the above-discussed methods for introducing variability into the shared secret "Km" (or distributing additional key material to increase the length of the shared secret) is employed to prevent the attacker from forcing the transmitter to employ the same shared secret value "Km" during both the encryption phase and decryption phase of the attack;

the transmitter is modified in accordance with the present invention so that it is not operable in any test mode that allows external control over the value "An," or each test mode in which the transmitter can be operated is modified to limit external control over the value "An" in some specific way. Preventing test mode operation entirely will typically be undesirable, because test modes serve a very useful purpose. However, test mode operation can be limited in either scope or in time to prevent many attacks of the described type. For example, the transmitter can be modified so that, if "An" were overwritten by an external agent, the HDCP state machines could allow authentication to proceed normally but would then intentionally scramble the resulting data. For another example, the video input to the transmitter is disabled during each test mode, and a test pattern is swapped in instead. Yet another example is to allow test mode operation only for a very short period of time (e.g., for some number of frames of input data), and then somehow "break" the link;

the encrypted data stream generated by the transmitter is "watermarked" or otherwise processed to make it difficult for an attacker to record it in a suitably loss-less way;

incorporate additional cryptography or other alterations in the process of encoding the encrypted data for transmission (e.g., the process of TMDS encoding of HDCP encrypted video data, in a system employing a DVI link to transmit the HDCP encrypted data) and decoding the encoded data at the receiver, to make it even more difficult for an attacker to suitably eavesdrop on the encrypted, encoded signal sent to the receiver by the transmitter;

incorporate analog circuitry in the circuitry employed to encode the encrypted data for transmission (e.g., the circuitry for TMDS encoding of HDCP encrypted video data, in a system employing a DVI link to transmit the HDCP encrypted data) and to decode the encoded data at the receiver, to make it easier to detect or inhibit eavesdropping on the encrypted, encoded signal sent to the receiver by the transmitter;

make variable the time delay that occurs while the transmitter transitions from a non-encrypting state into an encrypting state, and further ensure that such time delay will not be easily repeatable. This complicates the attacker's problem of obtaining the correct the timing for the second phase of the attack;

cause the transmitter to occasionally interrupt the normal timing or synchronization, either by re-authenticating or by temporarily disabling encryption (e.g., for a single frame on occasion). If this is done in a manner that is variable and difficult to repeat, it further complicates the attacker's problem of obtaining the correct the timing for the second phase of the attack;

test the data input to the transmitter (e.g., in data checking circuit 191 of transmitter 190 of Fig. 8) to detect whether an encrypted stream is being input, and if the test determines that the input data are encrypted, prevent the transmitter from further encrypting (i.e., decrypting) the encrypted input data stream. This can be done in any of a variety of ways. The transmitter can introduce into the encrypted stream to be transmitted a "header" of some kind that is easily distinguished (i.e., it could contain fields that specify the type and kind of encryption). Alternately, the transmitter can be implemented to examine the randomness of the data being input thereto. An encrypted video stream typically exhibits much more randomness than a normal video stream, and so could be distinguished in this way;

test the data input to the transmitter (e.g., in data checking circuit 191 of transmitter 190 of Fig. 8) to detect data that is obviously plain text (i.e., data that is indicative of any of one or more simple, predetermined patterns of values, for example, patterns consisting entirely of black values or white values), and prevent the transmitter from encrypting plain text; and

make it more difficult for the attacker to emulate a receiver's presence during the second phase (the decryption phase) of the attack. One method for doing this is to cause the transmitter always read the receiver's current "Ri" value first (before encrypting the next frame of data), which would require that the attacker provide such "Ri" values with proper timing. Another method for doing this is to implement the transmitter so that it keeps its own "Ri" values confidential (e.g., so that the transmitter does not reveal its own "Ri" values on the DDC bus of a DVI link, as is conventionally done in systems which send HDCP encrypted data over a DVI link), so that these values cannot be used by an attacker. Another method for making it more difficult for an attacker to emulate a receiver's presence during the decryption phase of an attack requires that the transmitter abort encryption or transmission of encrypted data unless status information is periodically transmitted to the transmitter (from a receiver) using a secure method (such as public-key cryptography). Still another method for making it more difficult for an attacker to emulate a receiver's presence during the decryption phase of an attack is to modify MSEN ("monitor sense") circuitry in each transmitter (and corresponding MSEN circuitry in each receiver), so that the modified MSEN circuitry in the transmitter can distinguish between a standard receiver and one capable of HDCP operation.